ABSTRACT OF THE DISCLOSURE

As fast algorithm for RSA cryptosystem, a calculation method employing the Chinese Remainder Theorem is widely used today. However, modular calculation modulo P (P: secret prime) has to be carried out in the first step of the calculation, and the modular calculation x mod P, explicitly using the secret prime P, has been used as the target of attack from long ago. To resolve the problem, there is provided a calculation method, in which x mod P is calculated not directly, but x*(2^n) mod P is calculated by previously multiplying x by 2^(m+n) mod P or 2^(2n) mod P and multiplying the result by 2^(-m) or 2^(-n) afterward. When Montgomery modular multiplication is used, subsequent process is carried out according to the conventional method. When a general modular multiplication method is used, the result of the modular exponentiation operation is corrected by multiplying the result by (2^(-n))^(2^n-1) mod P.